



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/007,859

11/13/2001

Mark C. Astley

GB920010085US1

7123

45541

7590

03/20/2008

HOFFMAN WARNICK & DALESSANDRO LLC

75 STATE ST

14TH FLOOR

ALBANY, NY 12207

EXAMINER

TOLENTINO, RODERICK

ART UNIT

PAPER NUMBER

2134

MAIL DATE

DELIVERY MODE

03/20/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/007,859	Applicant(s) ASTLEY ET AL.	
	Examiner Roderick Tolentino	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 December 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 13 November 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>12/22/2007</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1 – 16 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1 and 12 – 15, have been considered and are not persuasive.
3. Applicant's argue that that Gray in combination with Laage fail to disclose, teach or even suggest " performing an authentication check using the client data processing system's cipher-protected client password and the server data processing system's stored cipher-protected client password as a shared secret for said authentication check," as applied to claims 1 and 12 – 15. Examiner respectfully disagrees. Gray fails to teach performing an authentication check using the client data processing system's cipher-protected client password and the server data processing system's stored cipher-protected client password as a shared secret for said authentication check. However, in an analogous art Laage teaches performing an authentication check using the client data processing system's cipher-protected client password and the server data processing system's stored cipher-protected client password as a shared secret for said authentication check (Laage, Col. 10 Lines 50 – 57, hashes password to compare to hash value stored by server). Laage teaches a cleartext format of a password that is hashed, which is a form of ciphering, using a hash algorithm. The hash is also stored in the server database, NOT the cleartext password. Further on Column 10 lines 50 – 57 of Laage a comparison by the server of the stored hash and the hash of the input

password are compared to see if the password is valid. Which is an authentication check of 2 ciphered pieces of data as the limitations are written in the claim.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 9 and 12 – 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,844,497) in view of Laage et al. U.S. Patent No. (6,931,382).

6. As per claims 1 and 12 – 15, Gray teaches a process at the client data processing system applying the cipher function to the client password, which corresponds to the stored cipher-protected client password, thereby to generate a cipher-protected client password, which is equivalent to the stored cipher-protected client password (Gray, Col. 5 Lines 29 - 40, encrypted passwords), and the authentication check is adapted to be performed without having the client password in a cleartext format on the server data processing system (Gray, Col. 5 Lines 29 - 40, compares the encrypted passwords) wherein the authentication method is adapted to function without additional software infrastructure (Gray, Col. 5 Lines 29 - 40, no external software needed), but fails to teach performing an authentication check using

Art Unit: 2134

the client data processing system's cipher-protected client password and the server data processing system's stored cipher-protected client password as a shared secret for said authentication check. However, in an analogous art Laage teaches performing an authentication check using the client data processing system's cipher-protected client password and the server data processing system's stored cipher-protected client password as a shared secret for said authentication check (Laage, Col. 10 Lines 50 – 57, hashes password to compare to hash value stored by server).

At the time the invention was made, it could have been obvious to a person of ordinary skill in the art to use Laage's payment instrument authorization technique with Gray's method for providing an authentication system because it offers the advantage of checking to see if a password is actually valid (Laage, Col. 10 Lines 50 – 57).

7. As per claim 9, Gray discloses the server processing system's password repository is preferably integrated within the operating system of the server data processing system (Gray, Col. 6 Lines 9 - 21, OS works with verification system of passwords thus accessing all passwords associated to the system).

8. Claims 2 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,884,497) and Laage et al. U.S. Patent No. (6,931,382) and in further view of Boyko et al. U.S. Patent No. (7,047,408).

9. As per claim 2, Gray fails to teach an authentication check includes performing a mutual challenge-response authentication protocol check. However, in an analogous art

Jablon teaches an authentication check includes performing a mutual challenge-response authentication protocol check (Boyko, Col. 3 Lines 24 - 36).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Boyko's secure mutual network authentication with Gray's apparatus for providing an authentication system, because it offers the advantage of being a more secure.

10. As per claim 16, Gray as modified teaches generating a cipher-protected client password by applying said first cipher function to the client's password, thereby to provide the client and server processes with a shared secret (Boyko, Col. 3 Lines 24 - 36), generating a client response and counter-challenge to the server challenge, the client response and counter-challenge including a message authentication code computed using the cipher-protected client password (Boyko, Col. 3 Lines 24 - 36), forwarding the client response and counter-challenge to the server process ((Boyko, Col. 3 Lines 24 - 36) receiving the forwarded server response; generating an anticipated server response and comparing the received and anticipated server responses to determine whether they match; and in response to a positive match, confirming successful authentication (Boyko, Col. 3 Lines 24 - 36).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Boyko's secure mutual network authentication with Gray's apparatus for providing an authentication system, because it offers the advantage of being a more secure.

Art Unit: 2134

11. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,884,497) and Laage et al. U.S. Patent No. (6,931,382) and in further view of Patzer et al. U.S. Patent No. (6,732,270).

12. As per claim 3, Gray fails to teach the cipher function is an encryption algorithm wherein the cipher-protected client password comprises a salt and a character string. However, in an analogous art Patzer teaches the cipher function is an encryption algorithm wherein the cipher-protected client password comprises a salt and a character string (Patzer, Col. 4 Lines 18 - 31).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Patzer's method to authenticate a network access server to an authentication server with Gray's apparatus for providing an authentication system, because it offers the advantage of protecting against imposter clients (Patzer, Col. 2 Lines 16 -20).

13. Claims 6 – 8, are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,884,497) and Laage et al. U.S. Patent No. (6,931,382) and in further view of Davis et al. U.S. Patent No. (6,064,736).

14. As per claim 6, Gray fails to teach a hash function. However, in an analogous art Davis teaches a hash function (Davis, Col. 4, Lines 50 - 52).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Davis' password verification method and system with

Art Unit: 2134

Gray's apparatus for providing an authentication system, because it offers the advantage of protecting against unwanted users (Davis, Col. 2 Lines 15 - 26).

15. As per claim 7, Gray as modified teaches a process at the server data processing system retrieving from the repository the respective token for a stored cipher-protected client password, and transmitting the token to a client data processing system (Davis, Col. 5, Lines 11 - 14) and the process at the client data processing system applying the cipher function to the combination of the transmitted token and the client password which corresponds to the stored cipher-protected client password, thereby to generate the equivalent cipher-protected client password for use as a shared secret (Davis, Col. 5, Lines 18-31).

16. As per claim 8 Gray as modified teaches the token is a random number (Davis, Col. 5, Lines 11 - 13, salt).

17. Claims 4, 5 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,884,497) and Laage et al. U.S. Patent No. (6,931,382) and in further view of Yatsukawa U.S. Patent No. (6,148,404).

18. As per claim 4, Gray fail to teach an authentication check comprises generating a common secret session key at both the client and server data processing systems, using the generated encrypted client password at the client and the stored encrypted client password at the server, and using this common secret session key in a mutual challenge-response authentication protocol. However, Yatsukawa teaches an authentication check comprises generating a common secret session key at both the

client and server data processing systems, using the generated encrypted client password at the client and the stored encrypted client password at the server, and using this common secret session key in a mutual challenge-response authentication protocol (Yatsukawa, Col. 19, Lines 62 - 67).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Yatsukawa's common session-key with Gray's apparatus for providing an authentication system, because it offers the advantage of confidentiality by limiting the chance of leakage of information between client and server, along with unauthorized intrusion (Yatsukawa, Col. 1 Lines 35 - 42).

19. As per claim 5, Gray teaches a secret session key is generated by applying a cipher function to each of the generated encrypted client password at the client and the stored encrypted client password at the server (Yatsukawa, Col. 3, Lines 52 - 55).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Yatsukawa's common session-key with Gray's apparatus for providing an authentication system, because it offers the advantage of confidentiality by limiting the chance of leakage of information between client and server along with unauthorized intrusion (Yatsukawa, Col. 1 Lines 35 - 42).

20. As per claim 10, Gray as modified teaches the operating system is an operating system conforming to the UNIX operating system standard or derived from a UNIX conforming system (Yatsukawa, Col. 19, Lines 3 - 6).

21. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,884,497) and Yatsukawa U.S. Patent No. (6,148,404), as applied to claim 10.

22. As per claim 11, Gray fails to teach the encryption algorithm is provided by the UNIX crypt() function. However, in an analogous art Davis teaches the encryption algorithm is provided by the UNIX crypt() function (Davis, Col. 5, Lines 13 - 16).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Davis' password verification method and system with Gray's apparatus for providing an authentication system, because it offers the advantage of protecting against unwanted users (Davis, Col. 2 Lines 15 - 26).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Roderick Tolentino
Examiner
Art Unit 2134

Roderick Tolentino

/R. T./ 03/14/08

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134

